Publication number: JP10512428 (T)

Publication date: 1998-11-24

- international: *H04H1/00; H04H1/02; H04L9/00; H04N5/765; H04N5/92; H04N7/16; H04N7/167; H04N7/173;* H04H1/00; H04H1/02; H04L9/00; H04N5/765; H04N5/92; H04N7/16; H04N7/167; H04N7/173; (IPC1-7): H04H1/00; H04H1/02; H04L9/00; H04L9/10; H04L9/12; H04N5/765; H04N5/92; H04N7/16; H04N7/173

Application number: JP19960517183T 19961023

Priority number(s): EP19950202980 19951031; WO1996IB01137 19961023

Abstract not available for JP 10512428 (T)

Abstract of corresponding document: WO 9716924 (A1)

Translate this text

In a conditional access system, transmitted information is recorded in a scrambled form (SV). Accordingly, any access to the recorded information (SV) is subject to the condition that proper control word(s) (CW) are available. To enable access to the recorded information (SV), control word regeneration data (ECM, KRD) is stored. The proper control word(s) (CW) cannot easily be derived from this control word regeneration data (ECM, KRD). However security device (SCD) is capable of retrieving the proper control word(s) (CW) from the control word regeneration data (ECM, KRD). A system operator effectively masters operations carried out in the security device (SCD). Accordingly, if the system operator so desires, he may inhibit retrieval of the control word(s) (CW) and, consequently, prevent access to the recorded information (SV). The conditional access system may be used in, for example, pay-TV or multimedia purposes.

(19)日本国特許庁（ＪＰ）　(12) **公表特許公報（Ａ）**　(11)特許出願公表番号

特表平10－512428

(43)公表日　平成10年(1998)11月24日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｈ０４Ｎ	7/16		Ｈ０４Ｎ	7/16	Ｚ
Ｈ０４Ｈ	1/00		Ｈ０４Ｈ	1/00	Ｆ
	1/02			1/02	Ｆ
Ｈ０４Ｌ	9/00		Ｈ０４Ｎ	7/173	
	9/10			5/92	Ｈ

審査請求　未請求　　予備審査請求　未請求(全 25 頁)　最終頁に続く

(21)出願番号　特願平9－517183
(86)（22)出願日　平成８年(1996)10月23日
(85)翻訳文提出日　平成９年(1997)６月30日
(86)国際出願番号　ＰＣＴ／ＩＢ９６／０１１３７
(87)国際公開番号　ＷＯ９７／１６９２４
(87)国際公開日　平成９年(1997)５月９日
(31)優先権主張番号　９５２０２９８０．９
(32)優先日　1995年10月31日
(33)優先権主張国　オランダ（ＮＬ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＪＰ，ＫＲ

(71)出願人　フィリップス　エレクトロニクス　ネムローゼ　フェンノートシャップ
オランダ国　5621　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　1
(72)発明者　カンペルマン　フランシスカス　ルーカス　アントニウス　ヨハネス
オランダ国　5656　アーアー　アインドーフェン　プロフ　ホルストラーン　6
(74)代理人　弁理士　杉村　暁秀　（外６名）

(54)【発明の名称】　時間シフト限定アクセス

(57)【要約】
限定アクセスシステムにおいて、送信された情報を、スクランブルされた形態（ＳＶ）において記録する。したがって、記録された情報（ＳＶ）に対するどのようなアクセスも、適切な制御ワード（ＣＷ）が利用可能な状態を条件とする。記録された情報（ＳＶ）へのアクセスを可能にするために、制御ワード再生データ（ＥＣＭ，ＫＲＤ）を格納する。適切な制御ワード（ＣＷ）を、この制御ワード再生データ（ＥＣＭ，ＫＲＤ）から容易に得ることはできない。しかしながら、安全装置（ＳＣＤ）は、正確な制御ワード（ＣＷ）を制御ワード再生データ（ＥＣＭ，ＫＲＤ）から復元することができる。システムオペレータは、安全装置（ＳＣＤ）において行われる動作を実際に管理する。したがって、システムオペレータが望むなら、彼は、制御ワード（ＣＷ）の復元を禁止することができ、結果として、記録された情報（ＳＶ）へのアクセスを防止することができる。本限定アクセスシステムを、例えば、有料ＴＶまたはマルチメディア用途に用いることができる。

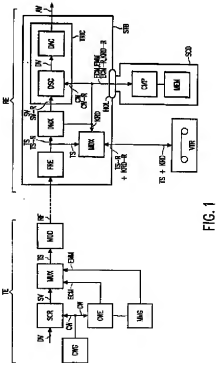

FIG. 1

【特許請求の範囲】

1．スクランブルされた情報（ＳＶ）を制御ワード（ＣＷ）に応じてデスクランブルされた情報（ＤＶ）に変換するデスクランブラ（ＤＳＣ）と、

前記デスクランブラ（ＤＳＣ）への前記制御ワード（ＣＷ）の供給を管理する安全装置（ＳＣＤ）とを具える限定アクセスシステムにおいて、

該限定アクセスシステムが、前記制御ワード（ＣＷ）と等しくない制御ワード再生データ（ＫＲＤ，ＥＣＭ）を、スクランブルされた情報（ＳＶ）の記録に関連して格納媒体（ＶＴＲ）に供給する手段（ＣＭＰ，ＭＥＭ）を具え、前記安全装置（ＳＣＤ）が、

前記記録されたスクランブルされた情報（ＳＶ－Ｒ）の前記デスクランブラ（ＤＳＣ）への供給に関連して、前記格納媒体（ＶＴＲ）から読み出した制御ワード再生データ（ＫＲＤ－Ｒ，ＥＣＭ－Ｒ）から制御ワード（ＣＷ－Ｒ）を復元する手段（ＣＭＰ，ＭＥＭ）を具えることを特徴とする限定アクセスシステム。

2．請求の範囲１に記載の限定アクセスシステムにおいて、前記制御ワード再生データ（ＫＲＤ，ＥＣＭ）を供給する手段（ＣＭＰ，ＭＥＭ）を、前記安全装置（ＳＣＤ）に結合したことを特徴とする限定アクセスシステム。

3．請求の範囲１に記載の限定アクセスシステムにおいて、前記安全装置（ＳＣＤ）を、前記制御ワード再生データを供給する手段（ＣＭＰ，ＭＥＭ）を制御する権利情報を受けるように結合したことを特徴とする限定アクセスシステム。

4．請求の範囲１に記載の限定アクセスシステムにおいて、前記安全装置（ＳＣＤ）を、前記制御ワードを復元する手段（ＣＭＰ，ＭＥＭ）を制御する権利情報を受けるように結合したことを特徴とする限定アクセスシステム。

5．請求の範囲１に記載の限定アクセスシステムにおいて、前記安全装置（ＳＣＤ）を分離可能とし、該システムが、前記分離可能な安全装置（ＳＣＤ）を保持するホルダ（ＨＯＬ）を含むことを特徴とする限定アクセスシステム。

6．制御ワード（ＣＷ）に応じてスクランブルされた情報（ＳＶ）をデスクランブルされた情報（ＤＶ）に変換するデスクランブラ（ＤＳＣ）への前記制御ワード（ＣＷ）の供給を管理する安全装置（ＳＣＤ）において、該安全装置がさら

に、

前記制御ワード（CW）と等しくない制御ワード再生データ（KRD，ECM）を供給する手段（CMP，MEM）と、

前記制御ワード再生データ（KRD，ECM）から前記制御ワード（CW）を復元する手段（CMP，MEM）とを具えることを特徴とする安全装置（SCD）。

7．スクランブルされた情報（SV）と、

前記スクランブルされた情報（SV）をデスクランブルする、制御ワード動作されるデスクランブラ（DSC）において使用するために、制御ワード（CW）の復元を可能にする制御ワード復元データ（KRD，ECM）とを具える記録媒体。

8．デスクランブラ（DSC）によって制御ワード（CW）に応じてデスクランブルされた情報（DV）に変換することができる送信されたスクランブルされた情報（SV）の時間シフトされた限定アクセスの方法において、

前記スクランブルされた情報（SV）を記録するステップと、

前記制御ワード（CW）と等しくない制御ワード再生データ（KRD，ECM）を格納媒体（VTR）に供給するステップと、

記録されたスクランブルされた情報（SV－R）を前記デスクランブラ（DSC）に供給するステップと、

前記格納媒体（VTR）から制御ワード再生データ（KRD，ECM）を読み出すステップと、

前記デスクランブラ（DSC）に供給するために、前記制御ワード再生データ（KRD，ECM）から前記制御ワード（CW）を復元するステップとを具える方法。

9．請求の範囲1に記載の限定アクセスシステムにおける送信の方法において、記録権利情報を前記安全装置に送信することを特徴とする方法。

【発明の詳細な説明】

時間シフト限定アクセス

本発明は、

－　スクランブルされた情報を制御ワードに応じてデスクランブルされた情報に変換するデスクランブラと、

－　前記デスクランブラへの前記制御ワードの供給を管理する安全装置とを具える限定アクセスシステムに関係する。

このようなシステムを、例えば、テレビジョン放送において使用し、特定のテレビジョンチャネル、または番組のみを、これらのサービスに対して料金を支払った視聴者に対してアクセス可能にする、すなわち、有料ＴＶを実現することができる。

１９９４年のSMPTE ジャーナルにおいて公表されたL.C.ギロウ（Guillou ）およびJ.-L. ギアチェッティ（Giachetti ）による記事“暗号化および限定アクセス”は、テレビジョン放送において使用する上述した形式の種々の限定アクセスシステムを記載している。既知のシステムにおいて、ビデオ信号をスクランブルされた形態において受信機に送信する。前記受信機は、デスグランブラを具え、このデスクランブラは、元のビデオ信号を復元するために前記送信信号をデスクランブルする。スクランブルおよびデスクランブルの双方を、制御ワードの制御の下で行う。使用するスクランブルアルゴリズムと共に前記制御ワードは、前記スクランブルされたビデオ信号と元のビデオ信号との関係を決定する。したがって、適切な制御ワードが利用可能ならば、前記スクランブルされたビデオ信号を、前記元のビデオ信号に変換し戻すことができるに過ぎない。したがって、受信端における前記元のビデオ信号へのアクセスは、前記制御ワードへのアクセスに制限される。

限定アクセスシステムの堅牢性を増すために、以下の手段を取る。第１に、前記制御ワードを定期的に変更する。第２に、前記制御ワードを、暗号化した形態において前記受信端に送信する。したがって、前記受信端は、前記元の制御ワードを復元する暗号復号器を具える。第３に、前記暗号復号器を、復号を行うため

に入力データとして鍵を必要とするような方法において実現する。前記鍵と共に、前記暗号復号器が従って動作する復号アルゴリズムは、前記元の制御ワードと暗号化された制御ワードとの関係を決定する。

前記SMPTE 記事の図２ないし５は、前述の３つの手段を使用する限定アクセスシステムの例を示す。前記SMPTE 記事の図２において、管理メッセージと呼ばれる暗号化された制御ワードを、毎月郵便によって受信端に送る。前記受けた暗号化された制御ワードを復号するのに使用する鍵を、分配鍵とする。前記分配鍵は、受信端毎に異なる。このように、図２において、前記暗号化された制御ワードと、この暗号化された制御ワードを暗号復号化する鍵の双方を、個人化する。

前記SMPTE 記事の図３、４および５に示すシステムにおいて、暗号化された制御ワードと、この制御ワードを暗号復号化する鍵とを、個人化しない。例えば、前記スクランブルされたビデオ信号と共に、前記暗号化された制御ワードを権利制御メッセージ（ＥＣＭ）の形態において送信することができる。これは、種々の受信端が、同じ暗号化された制御ワードを具える同じ権利制御メッセージＥＣＭを受信することを意味する。したがって、種々の受信端が、前記元の制御ワードを復元するのに同じ鍵を使用する。権利制御メッセージＥＣＭを復号する共通鍵を、許可鍵ＡＫと呼ぶ。許可鍵ＡＫおよび前記復号化アルゴリズムは、前記受信端における権利を表す。

許可鍵ＡＫを、暗号化された形態において、権利管理メッセージ（ＥＭＭ）として種々の受信端に送信する。受信端において、分配鍵を、権利管理メッセージＥＭＭを暗号復号化するのに使用する。分配鍵を、代表的に多様化する、すなわち、これらを、受信端毎か、受信端のグループ毎に異ならせる。したがって、権利管理メッセージを個人化することができる。加えて、“マスタ”の声を認識するために、権利管理メッセージの確実性を受信端において検査すべきである。前記“マスタ”を、例えば、スクランブルされたビデオ信号の放送者であるサービス提供者と呼ぶ。

前記SMPTE 記事の図３、４および５のシステムにおいて、制御ワードは一般に極めて多数のビット（代表的に６０ビット）と、短い寿命（代表的に１０秒）と

を有する。これは、１０秒毎に、権利制御メッセージＥＣＭの形態における新たな暗号化された制御ワードを，前記受信端に送信することを意味する。安全の理由のため、許可鍵ＡＫを、その度毎に変更する。許可鍵ＡＫを、暗号化された許可鍵ＡＫを伝達する権利管理メッセージＥＭＭによって更新する。

引用したSMPTE 記事に記載のシステムにおいて、各々の受信端は、安全装置を具える。前記安全装置は、受信端の権利に関する動作を行う、すなわち、有料ＴＶオペレータコマンドを実行する。前記動作は、暗号化された制御ワードの暗号復号化と、適切ならば、権利管理メッセージＥＭＭの暗号復号化とを含む。前記安全装置は、アクセスの権利を制限する状況に関係する他の動作を行ってもよい。このような状況は、例えば、予約期間、申込み前番組、一時的なアクセスに対する信用等である。

前記安全装置を、種々の方法において実現することができる。一般に、前記安全装置は、マイクロプロセッサを具える。前記安全装置を、前記デスクランブラに固定し、前記デスクランブラと集積し、１つのユニットを形成する。代わりに、前記安全カードをスマートカードとし、前記デスクランブラを具える受信ユニットから分離できるようにしてもよい。後者の選択は、前記制御ワードが多くのビットと十分に短い寿命とを有する場合、十分に安全である。どのような実現においても、前記安全装置を、安全のために、物理的にまたは電子的に偽造できないようにするべきである。

本発明の目的は、前記システムオペレータに、前記送信された情報のアクセスのより広範囲な制御を与える、上述した形式の限定アクセスシステムを提供することである。

本発明のある態様によれば、このようなシステムは、該システムが、

－　前記制御ワードと等しくない制御ワード再生データを、スクランブルされた情報の記録に関連して格納媒体に供給する手段を具え、前記安全装置が、

－　前記記録されたスクランブルされた情報の前記デスクランブラへの供給に関連して、前記格納媒体から読み出した制御ワード再生データから制御ワードを復元する手段を具えることを特徴とする。

本発明の他の態様は、実際的に、上記で規定した限定アクセスシステムに従っ

て、安全装置と、記録媒体と、時間シフト限定アクセスとに関係する。追加の特徴を、縦続の請求の範囲において規定する。

本発明は、前記SMPTE 記事が行わない、情報を守る時間シフトアクセスの機能を考慮する。引用したSMPTE 記事に記載のすべての限定アクセスシステムは、情報への、この情報の送信の時間における許可されないアクセス、すなわち短く直接アクセスを防ぐことに焦点をおいている。しかしながら、権利を与えられた受信端において、前記デスクランブルされた情報を、例えばテープに記録することができる。前記有料ＴＶオペレータは、前記記録された情報を実際に制御することができず、許可されない人物がこの記録された情報に自由にアクセスすることができる。

例えば、共同住宅において、スクランブルされたテレビジョン（ＴＶ）チャネルに予約した住人は、このチャネルにおける番組をデスクランブルされた形態において記録することができる。その後、彼は、この記録を、予約者ではないがこの番組を観たい他の住人に手渡すことができる。さらに、前記デスクランブルされた番組がダビング防止されていない場合、前記記録された番組による複製を物理的に防ぐことはできない。これらの複製を、例えば、その番組をいつでも好きなときに観るために前記関係するＴＶチャネルに予約する必要がないような種々の住人に配布することができる。

ディジタルテレビジョン放送の出現により、上述したことは有料ＴＶオペレータにとってより大きな問題になる。番組を、例えばＭＰＥＧ－２ディジタルビデオ信号として放送し、この番組のＭＰＥＧ－２ディジタルビデオ信号を記録する場合、この記録は、前記放送とほぼ同じ画像および音声品質を与える。どのようなダビング防止法も外した場合、前記番組を、どのような意味のある品質の劣化もなく、際限なく複製することができる。すなわち、有料ＴＶシステムにおける各々の受信端は、放送された有料ＴＶ番組の海賊版マスタの潜在的なオーナである。ディジタル有料ＴＶシステムにおいて、前記海賊版マスタは、前記有料ＴＶオペレータの公認マスタと同じ位またはほとんど同じ位良好である。

本発明による限定アクセスシステムにおいて、前記放送された情報は、前記システムオペレータが望む場合、依然として彼の制御の下にある。例えば、前記シ

ステムオペレータは、前記記録された情報にアクセスできる回数、前記記録された情報にアクセスできる期間、前記記録された情報にアクセスできる受信端、等を決定することができる。このように、本発明は、時間シフト情報アクセス機能を前記既知の限定アクセスシステムに付加すると同時に、この機能がこれらのシステムの安全性に影響を及ぼすことを回避する。

本発明のこれらのおよび他の態様および利点は、以下に記載の実施例の参照によって明らかになるであろう。

図１は、本発明による限定アクセスシステムの一実施例のブロック図である。

図２ａは、図１の限定アクセスシステムの第１の実現化における記録に関係する動作を説明する機能的な図である。

図２ｂは、図１の限定アクセスシステムの第１の実現化における再生に関係する動作を説明する機能的な図である。

図３ａは、図１の限定アクセスシステムの第２の実現化における記録に関係する動作を説明する機能的な図である。

図３ｂは、図１の限定アクセスシステムの第２の実現化における再生に関係する動作を説明する機能的な図である。

図４ａは、図１の限定アクセスシステムの第３の実現化における記録に関係する動作を説明する機能的な図である。

図４ｂは、図１の限定アクセスシステムの第３の実現化における再生に関係する動作を説明する機能的な図である。

本発明を、有料ＴＶシステムにおける用途を用いてより詳細に説明する。第１に、図１に示す有料ＴＶの機能要素を論考する。第２に、図１の有料ＴＶシステムの３つの実現化を論考し、これらの実現化においては、前記システムは異なって動作する。図２ａ、２ｂ、図３ａ、３ｂおよび図４ａ、４ｂは、これら３つの個々の実現化における動作を説明する。第３に、本発明によって与えられる有料ＴＶシステムにおける有利な効果を強調する。第４に、いくつかの代わりの実施例を取り扱い、請求した本発明の範囲が以下に例として与える有料ＴＶシステムを十分に越えることを示す。

図２の有料ＴＶシステムにおいて、送信端ＴＥは、有料ＴＶ番組をスクランブ

ルされた形態において、受信端ＲＥに伝送する。受信端ＲＥは、ビデオテープレコーダＶＴＲを有し、どのような送信された有料ＴＶ番組も送信時より後の時間において観ることができる。これをさらに、時間シフトされた視聴と呼ぶ。前記受信端は、以下のユニット、すなわち、セットトップボックスＳＴＢと、分離可能安全装置ＳＣＤ、例えばスマートカードとをさらに具える。セットトップボックスＳＴＢは、物理的および電気的に安全装置ＳＣＤを結合するホルダＨＯＬを有する。

送信端ＴＥにおいて、スクランブル化装置ＳＣＲは、ビデオ信号ＤＶ、例えばＭＰＥＧ－２符号化ビデオ信号をスクランブルし、スクランブルされたビデオ信号ＳＶを得る。前記スクランブル化は、制御ワードＣＷに依存し、この制御ワードＣＷを制御ワード発生器ＣＷＧによって発生する。このために、ディジタルビデオ信号ＤＶとスクランブルされたビデオ信号ＳＶとの関係は、制御ワードＣＷと使用されるスクランブル化アルゴリズムとによって決定される。制御ワード発生器によって与えられる制御ワードＣＷを、例えば、１０秒毎に周期的に変化させる。

制御ワード暗号器ＣＷＥおよび管理メッセージ発生器ＭＭＧは、受信端ＲＥにおけるデスクランブル化に必要なデータを与える。さらに特に、制御ワード暗号器ＣＷＥは、制御ワードＣＷを暗号化した形態において与え、これらのワードを、権利制御メッセージＥＣＭに含める。管理メッセージ発生器ＭＭＧは、許可鍵ＡＫを暗号化された形態において与え、この鍵を権利管理メッセージＥＭＭに含める。許可鍵ＡＫは、権利制御メッセージＥＣＭから制御ワードを復元するのに必要である。

権利制御メッセージＥＣＭは、少なくとも制御ワードＣＷにおける変化と同じくらい頻繁に変化する。例えば、１０秒毎に、新たな制御ワードＣＷを具える権利制御メッセージＥＣＭが、前記受信端に伝送される。しかしながら、制御ワードＣＷをデスクランブルする許可鍵ＡＫは、制御ワードＣＷよりかなり間を置いて、例えば、１週間または１か月に一度のみ変化する。したがって、権利管理メッセージＥＭＭは、権利制御メッセージＥＣＭよりかなり頻度が少ない。したがって、テレビジョン番組中、例えば、多数の権利制御メッセージＥＣＭが受信端

ＲＥに伝送されるが、権利管理メッセージＥＭＭはまったく伝送されない。

マルチプレクサＭＵＸは、スクランブルされたビデオ信号ＳＶと、権利制御メッセージＥＣＭおよび権利管理メッセージＥＭＭとを、１つの輸送ストリームに結合する。輸送ストリームＴＳを変調器ＭＯＤに供給し、変調器ＭＯＤは、送信信号ＲＦを与える。

受信端ＲＥにおけるセットトップボックスＳＴＢは、以下の機能的部分、すなわち、フロントエンドＦＲＥ、デマルチプレクサＤＭＸ、マルチプレクサ／デマルチプレクサＭＤＸ、デスクランブラＤＳＣおよびアナログーディジタル（Ａ／Ｄ）コンバータＡＤＣを具える。フロントエンドＦＲＥは、送信信号ＲＦから輸送ストリームＴＳを得る。輸送ストリームＴＳをデマルチプレクサＤＭＸに供給し、このデマルチプレクサＤＭＸは、輸送ストリームＴＳに含まれる種々の形式の情報を分離する。したがって、スクランブルされたビデオ信号ＳＶは、権利制御メッセージＥＣＭおよび権利管理メッセージＥＭＭから分離される。マルチプレクサ／デマルチプレクサＭＤＸは、ビデオテープレコーダＶＴＲに対するインタフェースである。以下により詳細に論考する。

デスクランブラＤＳＣは、スクランブルされたビデオ信号ＳＶを受け、安全装置ＳＣＤから制御ワードＣＷを受ける。適切な制御ワードＣＷによって、デスクランブラＤＳＣは、スクランブルされたビデオ信号ＳＶをディジタルビデオ信号ＤＶに変換し、このディジタルビデオ信号ＤＶは、前記送信端においてスクランブラＳＣＲに供給されたものである。ディジタルーアナログ（Ｄ／Ａ）コンバータＤＡＣは、ディジタルビデオ信号ＤＶを、画像表示装置（図示せず）に供給するのに適切なアナログビデオ信号ＡＶに変換する。デスクランブラＤＳＣおよびＤ／Ａコンバータ ＤＡＣを，偽造防止集積回路ＴＲＩＣに収容する。したがって、ディジタルビデオ信号ＤＶに容易にアクセスできないため、どのような有料ＴＶ番組のディジタル記録も妨げられる。

安全装置ＳＣＤは、デマルチプレクサＤＭＸによって供給される権利制御メッセージＥＣＭおよび権利管理メッセージＥＭＭを暗号復号化する。権利管理メッセージＥＭＭの暗号復号化は、許可鍵ＡＫを与え、この許可鍵ＡＫは、権利制御メッセージＥＣＭおよび／または受信端ＲＥの権利に関する他のデータを暗号復

号化するのに必要である。権利制御メッセージＥＣＭの暗号復号化は、制御ワードＣＷを与え、この制御ワードＣＷは、ディジタルビデオ信号ＤＶを復元するためにデスクランブラＤＳＣが必要とする。

安全装置ＳＣＤは、上述した動作を行い、その結果を格納する、マイクロコンピュータＣＭＰおよびメモリＭＥＭを具える。メモリＭＥＭは、最新の権利制御メッセージＥＣＭから得られた現在の制御ワードＣＷを格納することができる書き込み可能部分を有する。さらに、権利制御メッセージＥＣＭを暗号復号化する許可鍵ＡＫを、新たな権利管理メッセージＥＭＭを受けるまで、前記書き込み可能部分に格納する。メモリＭＥＭは、さらに、例えば、暗号復号化アルゴリズムを格納する読み出し専用部分を有してもよい。

ビデオテープレコーダＶＴＲは、マルチプレクサ／デマルチプレクサＭＤＸから、記録するための入力信号を受ける。この入力信号は、輸送ストリームＴＳを具える。このように、ビデオテープレコーダＶＴＲは、スクランブルされた形態におけるどのような有料ＴＶ番組も、付随する権利制御メッセージと共にディジタル式に記録することができる。記録された有料ＴＶ番組を再生する場合、記録された輸送ストリームＴＳ－Ｒを、マルチプレクサ／デマルチプレクサＭＤＸを経てデマルチプレクサＤＭＸに供給する。したがって、デマルチプレクサＤＭＸは、記録された権利制御メッセージＥＣＭ－Ｒを安全装置ＳＣＤに供給し、記録されたスクランブルされたビデオ信号ＳＶ－Ｒをデスクランブラ ＤＳＣに供給する。

しかしながら、輸送ストリームＴＳのみを記録した場合、記録された有料ＴＶ番組を観ようとすると、以下の問題が生じる。記録された有料ＴＶ番組を再生する時間において、記録が行われた時間から権利管理メッセージＥＭＭが安全装置ＳＣＤに伝送されてしまっているかもしれない。その場合において、記録の時間中に変化する許可鍵ＡＫは、新たな許可鍵ＡＫに置き換えられている。結果として、安全装置ＳＣＤは、供給された記録された権利制御メッセージＥＣＭ－Ｒから適切な制御ワードＣＷを復元することができない。

図１の有料ＴＶシステムにおいて、安全装置ＳＣＤは、有料ＴＶ番組が記録された場合、鍵関連データＫＲＤを与える。鍵関連データＫＲＤを、マルチプレク

サ／デマルチプレクサＭＤＸにおいて輸送ストリームＴＳに結合し、続いてビデオテープレコーダＶＴＲに供給する。記録された有料ＴＶ番組を再生する場合、記録された鍵関連データＫＤＲ－Ｒは、マルチプレクサ／デマルチプレクサＭＤＸを経て安全装置ＳＣＤに戻る。安全装置ＳＣＤは、鍵関連データＫＲＤを使用して、前記記録の時間において変化した許可鍵を再インストールする。したがって、記録された権利制御メッセージＥＣＭ－Ｒを暗号復号化することができ、結果として、前記記録に適合した制御ワードＣＷ－Ｒを再生中にデスクランブラＤＳＣに供給することができる。

図１の有料ＴＶの、鍵関連データＫＲＤが性質において異なる３つの実現化を以下に説明する。しかしながら、３つの実現化のすべては共通して、だれか許可されない人物が鍵関連データＫＲＤから適切な許可鍵ＡＫを得ることは、可能であっても困難である。

図２ａおよび２ｂは、図１の有料ＴＶシステムの第１の実現化における、安全装置ＳＣＤにおいて行われる動作を説明する。図２ａにおいて、有料ＴＶ番組をその送信の時間において視るために必要な動作を、比較的細い線によって示す。安全装置ＳＣＤに伝送される権利管理メッセージＥＭＭの暗号復号化ＤＭＭは、許可鍵ＡＫを与える。許可鍵ＡＫのメモリＭＥＭへの書き込みＷＫＴは、少なくとも新たな権利管理メッセージＥＭＭが伝送されるまで、安全装置ＳＣＤにおいて許可鍵ＡＫを利用可能にする。許可鍵ＡＫのメモリＭＥＭからの読み出しＲＫＴによって、許可鍵ＡＫを権利制御メッセージＥＣＭの暗号復号化ＤＣＭにおいて使用する。暗号復号化ＤＣＭは、図１に示すデスクランブラＤＳＣにおけるスクランブルされたビデオ信号ＳＶをデスクランブルするのに必要な適切な制御ワードＣＷを与える。

図２ａにおいて、有料ＴＶ番組の記録に関係するこれらの動作を、太線において示す。有料ＴＶ番組の記録の確認ＩＲＣは、許可鍵ＡＫの暗号化ＥＡＫに関する条件であり、この鍵を、メモリＭＥＭから読み出しＲＫＥによって読み出す。暗号化された許可鍵Ｅ（ＡＫ）は、図１に示すような輸送ストリームＴＳと共にビデオテープレコーダＶＴＲにおいて記録された鍵関連データＫＲＤを構成する。記録された有料番組を再生する場合、図１における鍵関連データＫＲＤ－Ｒに

相

当する記録された暗号化許可鍵Ｅ（ＡＫ）－Ｒを、マルチプレクサ／デマルチプレクサＭＤＸを経て安全装置ＳＣＤに供給する。

図２ｂは、記録された有料ＴＶ番組を観るために行われるこれらの動作を説明する。暗号復号化ＤＡＫは、暗号化された許可鍵Ｅ（ＡＫ）から記録許可鍵ＡＫ－Ｒを復元する。記録許可鍵ＡＫ－Ｒは、記録された有料ＴＶ番組の送信時においてメモリＭＥＭにおいて存在する許可鍵ＡＫに等しい。メモリＭＥＭへの記録許可鍵ＡＫ－Ｒの書き込みＷＫＲは、安全装置ＳＣＤにおいて記録許可鍵ＡＫ－Ｒを、少なくとも記録された有料ＴＶ番組の複聴が終了するまで利用可能にする。時間シフト視聴の確認ＩＴＳは、メモリＭＥＭからの記録許可鍵ＡＫ－Ｒの読み出しＬＲＫＲの条件である。記録ＲＫＲにより、記録許可鍵ＡＫ－Ｒを、記録された権利制御メッセージＥＣＭ－Ｒの暗号復号化ＤＣＭにおいて使用する。図２ｂにおける暗号復号化ＤＣＭは、記録されたスクランブルされたビデオ信号ＴＳ－Ｒをデスクランブルする制御ワードＣＷ－Ｒをあたえる。

図３ａおよび３ｂは、図１の有料ＴＶシステムの第２の実現化において、安全装置ＳＣＤにおいて行われる動作を説明する。図３ａにおける比較的細い線による動作は、図２ａにおけるこれらと同じである。図３ａにおいて、許可鍵ＡＫの複製ＣＫＴを、メモリＭＥＭにおいて、有料ＴＶ番組の記録ＩＲＣの確認に応じて行う。したがって、複製された許可鍵ＡＫ－Ｃは、、ＭＥＭにおいて存在する。許可鍵ＡＫとは違って、複製された許可鍵ＡＫ－Ｃは、原則的には、新たな権利管理メッセージＥＭＭが安全装置ＳＣＤに伝送された場合、上書きされない。ラベル発生ＬＡＧは、アドレスＡＤを、複製された許可鍵ＡＫ－Ｃをメモリ ＭＥＭに格納するのに従って、ラベルＬＡＢに変換する。ラベルＬＡＢは、鍵関連データＫＲＤを構成し、これは、図１において示すような輸送ストリームＴＳと共に記録されたものである。記録された有料ＴＶ番組を再生する場合、図１における記録された鍵関連データＫＲＤ－Ｒに等しい記録されたラベルＬＡＢ－Ｒを、マルチプレクサ／デマルチプレクサＭＤＸを経て安全装置ＳＣＤに供給する。

図３ｂは、記録された有料ＴＶ番組の再生に関係する動作を説明する。ラベル

解釈ＬＡＩは、復製された確認鍵ＡＫをメモリＭＥＭに格納するのに従って、アドレスＡＤを復元する。時間シフトされた視聴ＩＴＳの確認を条件として、復製

された許可鍵ＡＫ－Ｃの読み出しＲＫＣを行う。読み出しＲＫＣにより、復製された許可鍵ＡＫ－Ｃを、記録された権利制御メッセージＥＣＭ－Ｒの暗号復号化ＤＣＭにおいて使用する。図３ｂにおける暗号復号化ＤＣＭは、制御ワードＣＷ－Ｒを与え、これは、記録されたスクランブルされたビデオ信号ＳＶ－Ｒをデスクランブルするのに適切である。

図４ａおよび４ｂは、図１の有料ＴＶシステムの第３の実現化において、安全装置ＳＣＤにおいて行われる動作を説明する。図４ａにおける比較的細い線による動作は、図２ａにおけるこれらと同じである。図４ａにおいて、安全装置ＳＣＤに伝送された権利管理メッセージＥＭＭのメモリＭＥＭへの書き込みＷＭＭを行う。したがって、権利管理メッセージＥＭＭを、安全装置ＳＣＤのメモリＭＥＭに格納する。これは、標準的な慣習ではないことに注意されたい。通常、権利管理メッセージＥＭＭの暗号復号化ＤＭＭの結果を格納し、この結果は許可鍵ＡＫを与えるが、権利管理メッセージＥＭＭそれ自身は格納しない。有料ＴＶ番組の記録の確認ＩＲＣの状態を条件として、メモリＭＥＭに格納された権利管理メッセージＥＭＭの読み出しＲＭＭを行う。読み出しＲＭＭにより、権利管理メッセージＥＭＭを、鍵関連データＫＲＤとして、図１に示すマルチプレクサ／デマルチプレクサＭＤＸに供給し、結果として、権利管理メッセージＥＭＭを、輸送ストリームＴＳと共に記録する。

図４ｂは、記録された有料ＴＶ番組を再生するために行う動作を説明する。有料ＴＶ番組の時間シフトされた視聴ＩＴＳの確認の状態を条件として、記録された権利管理メッセージＥＭＭ－Ｒの暗号復号化ＤＭＭを行う。暗号復号化ＤＭＭは、記録された権利管理メッセージＥＭＭ－Ｒから記録許可鍵ＡＫ－Ｒを復元する。図４ｂに示す他の動作は、図２ｂに示すこれらと同じである。

以下の意見は、３つの上述した実現化に関するものである。第１に、図２ｂ、３ｂおよび４ｂに示す暗号復号化ＤＣＭは、図２ａ、３ａおよび４ａに示すこれらと、動作において同じである。これらを実行する瞬間、すなわち、関連した有

料ＴＶ番組の、各々、再生中か、送信中かのみが異なっている。

第２に、図２ａおよび２ｂと図４ａおよび４ｂとに各々示す第１および第３の実現化において、許可鍵ＡＫを、暗号化された形態において、安全装置ＳＣＤの外部に格納する。前記第１の実現化において、許可鍵ＡＫを、安全装置ＳＣＤにおいて暗号化する。記録鍵を、許可鍵ＡＫを暗号化するのに使用することができ、この記録鍵を、安全装置ＳＣＤに固有のものとしてもよい。前記第３の実現化において、権利管理メッセージＥＭＭになる、送信端における許可鍵ＡＫの暗号化を有効に使用する。このように、図４ｂに示す鍵関連データＫＲＤの暗号復号化ＤＭＭは、図４ａにおける暗号復号化ＤＭＭと同じである。

第３に、上述した実現化において記録することを権利に含め、どのような有料ＴＶ番組の記録も許可するまたは禁止するようにすることができる。例えば、安全装置ＳＣＤによる鍵関連データＫＲＤの出力を、受信端ＲＤが関連する有料ＴＶ番組を記録する権利を与えられる状態を条件として行うことができる。これは、送信の瞬時において有料ＴＶ番組を視聴する権利を除く、すなわち、時間シフトされた視聴のみが禁止される。例えば、送信端ＴＥは、記録権利を、直接の視聴権利と同様にすなわち、権利管理メッセージＥＭＭによって伝送することができる。

第４に、時間シフトされた視聴の表示ＩＴＳを、輸送ストリームＴＳにおける時間スタンプされたメッセージから得ることができる。例えば、権利管理メッセージＥＣＭが、このようなタイムスタンプされたメッセージを具えてもよい。したがって、時間チェック機能を、図１の有料ＴＶシステムに与える。安全装置ＳＣＤに内部クロックを設けた場合、直接視聴に関する輸送ストリームＴＳか、時間シフトされた視聴に関する輸送ストリームＴＳ－ＲかのどちらがセットトップボックスＳＴＢにおいて処理されているかを区別することができる。さらに、前記記録の年齢を決定することができ、この情報を使用して、視聴を許可するかまたは許可しないかを決定することができる。

第５に、輸送ストリームＴＳは、それが由来するところのものから有料ＴＶ番組を識別するデータを具えてもよい。例えば、権利制御メッセージＥＣＭは、ど

の有料ＴＶ番組がこれらの権利制御メッセージＥＣＭと多重化されているかを区別するデータを含んでもよい。この場合、安全装置ＳＣＤは、受けた権利制御メッセージＥＣＭから、どの有料ＴＶ番組がデスクランブラＤＳＣに供給されているかを決定することができる。

上述した有料ＴＶシステムにおいて用いた本発明は、有料ＴＶオペレータが、実際に、記録された有料ＴＶ番組の“マスタ”であるという利点を与える。これは、有料ＴＶオペレータが、彼がそう望む場合、記録された有料ＴＶ番組のどのような視聴も禁止できることを意味する。記録された有料ＴＶ番組を視聴するために必要な制御ワードＣＷ－Ｒを、安全装置ＳＣＤにおいて、記録された権利制御メッセージＥＣＭ－Ｒと、記録された鍵関連データＫＲＤ－Ｒとから復元する。前記ＴＶオペレータは、安全装置ＳＣＤにおける動作を制御する者である。したがって、彼は、適切な制御ワードＣＷ－ＲをデスクランブラＤＳＣに供給するために満たされなければならない条件を与えてもよい。

例えば、有料ＴＶオペレータは、以下の方法において、記録された有料ＴＶ番組を観ることが出来る回数を決定することができる。有料ＴＶオペレータは、権利管理メッセージＥＭＭを安全装置ＳＣＤに伝送し、条件“記録された有料ＴＶ番組の視聴は５回以下”を設定することができる。視聴の回数を計数するために、安全装置ＳＣＤは、番組識別および計数用ソフトウェアを具えてもよい。安全装置ＳＣＤが、有料ＴＶ番組が６回目の視聴であることを確立した場合、デスクランブラＤＳＣへの制御ワードＣＷ－Ｒの供給を禁止する。

有料ＴＶオペレータが与えることができる他の条件は、有料ＴＶ番組を観ることが出来る期間である。再び、この条件を、権利管理メッセージＥＭＭによって、安全装置ＳＣＤに伝送してもよい。安全装置ＳＣＤは、安全装置ＳＣＤに供給された番組の年齢を決定するソフトウェアを具えてもよい。例えば、権利制御メッセージＥＣＭに含まれる上述したタイムスタンプされたメッセージを、この目的のために使用することができる。

本発明は、さらに、原則的に、記録された有料ＴＶ番組を、記録に使用された安全装置ＳＣＤが利用可能な場合にのみ視聴することができるという利点を与え

る。輸送ストリームＴＳと共にテープに記録された鍵関連データＫＲＤのみが、この鍵関連データＫＲＤを発生した安全装置に対して意味がある。記録された有料ＴＶ番組を再生する場合、他の安全装置ＳＣＤが、鍵関連データＫＲＤから適切な許可鍵ＡＫを得る可能性は、除外されないとしても非常に成功しそうにない。したがって、図１に示す受信端ＲＥの所有者が、彼の友人にテープに記録された

有料ＴＶ番組を貸した場合、前記所有者が彼の安全装置ＳＣＤも彼の友人に貸した場合のみ、この友人は前記有料ＴＶ番組を観ることができる。前記所有者が彼の安全装置ＳＣＤを貸さない場合、問題の友人は、有料ＴＶオペレータに、彼に視聴する権利を与えることを要求しなければならない。

加えて、本発明は、記録された有料ＴＶ番組が版権保護されるという利点を与える。記録された有料ＴＶ番組のどのような複製も、オリジナルを記録するのに使用された安全装置が利用可能である場合にのみ観ることができることは、上記から明らかであろう。

まとめにおいて、本発明は、有料ＴＶシステムに時間シフトして視聴する機能を与え、同時にこの機能が前記有料ＴＶシステムの安全性に実際的に影響を及ぼすのを回避する。

例として与えたこれら以外の多数の実施例および実現化も、請求した本発明の範囲内であることは明らかであろう。

許可鍵ＡＫ以外の限定アクセスデータを、上述した実施例における許可鍵ＡＫと同様に処理することができる。このような限定アクセスデータは、例えば、一般的に指定される許可鍵ＡＫを、受信端ＲＥにおける権利付与に使用することの正当性に関係してもよい。図２ａを参照すると、権利付与を、鍵関連データＫＲＤおよび輸送ストリームＴＳを図１に示すビデオテープレコーダＶＴＲにおいて記録するために、安全装置ＳＣＤにおいて暗号化することができる。

機能的要素を種々のユニットへ物理的に分布させる多数の方法が存在する。図１は、極めて図式的であり、本発明による条件アクセスシステムの１つの可能な実施例を表しているに過ぎない。例えば、図１に示す条件アクセスシステムのす

べての機能的要素を、ビデオテープレコーダＶＴＲに統合してもよい。代わりの実施例において、安全装置ＳＣＤを、ビデオテープレコーダＶＴＲから分離可能なスマートカードとして実現することができる。他の代わりの実施例において、安全装置ＳＣＤを、セットトップボックスＳＴＢに統合してもよい。これらを、記録のための専用のユニットと、他の目的のための他のユニットとしてもよい。

鍵関連データＫＲＤを輸送ストリームＴＳと共にビデオテープレコーダＶＴＲにおいて格納する代わりに、鍵関連データＫＲＤをどこか他に格納してもよい。

例えば、鍵関連データＫＲＤを、セットトップボックスＳＴＢに結合したメモリ（図示せず）に格納することができる。もちろん、この実施例において、セットトップボックスＳＴＢに格納された鍵関連データＫＲＤを記録された有料ＴＶ番組にリンクする設備を形成しなければならない。

ビデオテープレコーダＶＴＲの代わりに、なにか他の記録媒体、例えば、光または磁気ディスクを使用してもよい。本発明を、別個のハードウェアによって、または適切なソフトウェアによって供給されるプロセッサによって実現することができる。請求の範囲におけるどのような参照符も、関連する請求の範囲を制限すると解釈すべきではない。限定アクセスシステムにおいて、送信された情報を、スクランブルされた形態ＳＶにおいて記録する。したがって、記録された情報ＳＶに対するどのようなアクセスも、適切な制御ワードＣＷが利用可能であるという状態を条件とする。記録された情報ＳＶへのアクセスを可能にするために、制御ワード再生データＥＣＭ、ＫＲＤを格納する。適切な制御ワードＣＷを、この制御ワード再生データＥＣＭ、ＫＲＤから容易に得ることはできない。しかしながら、安全装置ＳＣＤは、制御ワード再生データＥＣＭ、ＫＲＤから適切な制御ワードＣＷを復元することができる。システムオペレータは、安全装置ＳＣＤにおいて行われる動作を実際に管理する。したがって、システムオペレータがそう望むなら、彼は、制御ワードＣＷの復元を禁止することができ、したがって、記録された情報へのアクセスを防止することができる。

【図１】

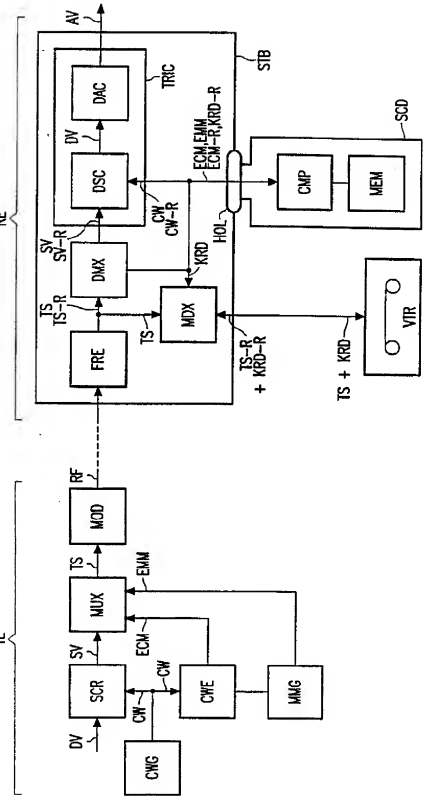
TE
RE
CWG
DV
SCR
SV
CW
CWE
ECM
MMG
MUX
TS
EMM
MOD
RF
FRE
TS
TS-R
DMX
SV
SV-R
KRD
MDX
TS
TS-R
+ KRD-R
DSC
CW
CW-R
ECM,EMM
ECM-R,KRD-R
HOL
DV
DAC
AV
TRIC
STB
CMP
MEM
SCD
TS + KRD
VTR

FIG. 1

【図２】

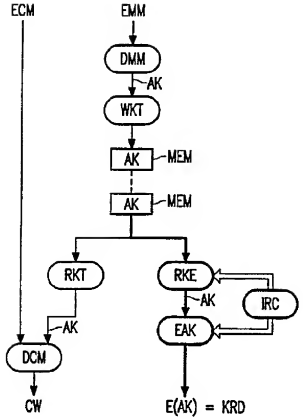

FIG. 2a

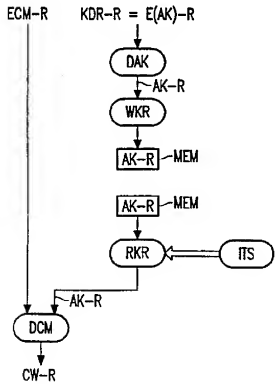

FIG. 2b

【図３】

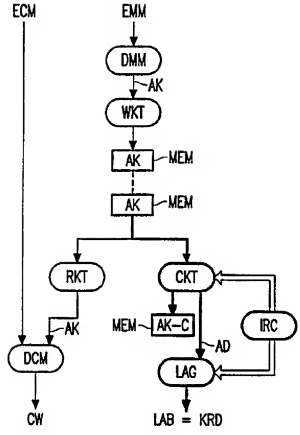

FIG. 3a

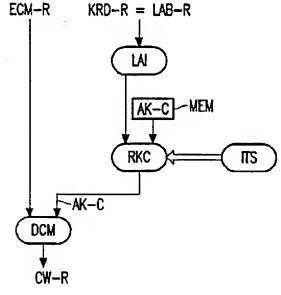

FIG. 3b

【図４】

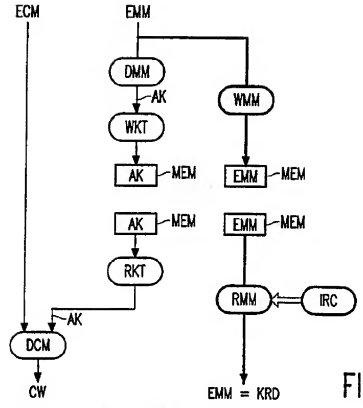

FIG. 4a

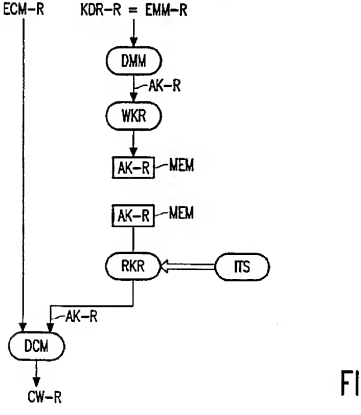

FIG. 4b

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 96/01137

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04N 7/167, H04K 1/04
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04K, H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2132860 A (BRITISH BROADCASTING), 11 July 1984 (11.07.84), figure 1, abstract	1
A	--	2-5

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 February 1997	21 -02- 1997
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT
Information on patent family members

03/02/97

International application No.
PCT/IB 96/01137

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB-A- 2132860	11/07/84	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(51)Int.Cl.[6]		識別記号	FI		
H04L	9/12		H04N	5/91	L
H04N	5/765		H04L	9/00	
	5/92				Z
	7/173				